Universal Blind Quantum Computation

Anne Broadbent (Institute for Quantum Computing, University of Waterloo)
with
Joseph Fitzsimons (Oxford)
Elham Kashefi (Edinburgh)
The year is 20???. A few centers around the world have managed to build quantum computers.

They allow users to have remote access to their quantum computers.
How can Alice be convinced that the output provided by the quantum computer is correct?

Can she do this while keeping her input private?
Interactive proofs

...how useful is a cheating oracle?
A language $L$ is in $\text{IP}$ if there exists a verifier such that:

- If the answer is "yes", the prover must be able to behave in such a way that the verifier accepts with probability at least $2/3$.

- If the answer is "no", then however the prover behaves, the verifier must reject with probability at least $2/3$.

$\text{IP} = \text{PSPACE}$ (Shamir, Lund-Fortnow-Karloff-Nisan 1990)
A language $L$ is in $\text{QIP}$ if there exists a verifier such that:
• If the answer is "yes," the prover must be able to behave in such a way that the verifier accepts with probability at least 2/3
• If the answer is "no," then however the prover behaves the verifier must reject with probability at least 2/3.

• $\text{PSPACE}$ is in $\text{QIP}[3]$ (Watrous 1999)
• $\text{QIP}[k] = \text{QIP}[3] = \text{QIP}$ ($k \geq 3$) (Kitaev-Watrous 2000).

• Open question: Does $\text{QIP}$ strictly contain $\text{IP}$ (i.e. does quantum computation add any power to interactive proofs?)
Limiting the quantum prover

- Open question: what is the power of this type of scenario?
  \[ \text{IP}_{BQP} \overset{?}{=} BQP \]

- Our contribution: we give solutions to closely related problems:
  1. Almost-classical verifier (has the additional power of generating random qubits from a fixed finite set):
     \[ \text{IP}_{BQP}^{(\theta)} = BQP \]
  2. Purely classical verifier, with \textbf{two} BQP provers that cannot communicate but that share entanglement
     \[ \text{MIP}^*_{BQP} = BQP \]

Major open problem: characterize the power of MIP*.
Cryptography

...what can be accomplished in the presence of an adversary?
Cryptography

- Quantum key distribution (QKD) (Bennett-Brassard 1984)
- Impossibility of Bit Commitment (Mayers, Lo-Chau 1995)
- Private Quantum Channels (Ambainis-Mosca-Tapp-de Wolf 2000)
- Quantum Authentication (Barnum-Crépeau-Gottesman-Smith-Tapp 2002)
- Multi-party computation (Ben-Or-Crépeau-Gottesman-Hassidim-Smith 2006)
- Cryptography in the bounded quantum-storage model (Damgard-Fehr-Salvail-Schaffner 2005)
Our protocol achieves perfect privacy & detection of interfering Bob;
It can also be used for quantum inputs or outputs
Motivations

- **Factoring**
  - Using Shor’s algorithm, Alice can use Bob to help her factor an integer corresponding to an RSA public key
    - Bob won’t learn whose private key he is breaking; in fact he won’t even know that he is helping Alice factor.

- **BQP-Complete problem**
  - No known efficient method to verify solution: we therefore give a method to authenticate Bob’s computation.

- **Processing quantum information**
  - Blind state preparation, blind measurement...
Previous work

- Publicly-known classical random-verifiable function
- Alice needs to be able to prepare and measure multi-qubit states
- Provides only cheat sensitivity
Alice needs a **quantum memory**, and the ability to perform Pauli gates

\[ x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad z = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \]

Idea: she sends encrypted qubits to Bob who applies a known gate. Alice can decrypt the qubits while preserving the action of the gate. Repeat, cycling through universal set of gates.

\[ H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \pi/8 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{i} \end{pmatrix}, \quad CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \]
Interactive proof with BQP prover, and nearly-classical verifier.

- Verifier has a constant-size quantum computer
- Protocol is also *blind*. 

**Interactive Proofs For Quantum Computations**

Dorit Aharonov* Michael Ben-Or* Elad Eban*

October 29, 2008
Our solution

Blind protocols that show:

\[ BQP = IP_{BQP}^{|\theta)} \]
\[ BQP = MIP_{BQP}^* \]
High-level protocol

- Prepares qubits randomly chosen in
  \[ \frac{1}{\sqrt{2}} (|0\rangle + e^{i\theta}|1\rangle) \quad \theta \in \{\frac{n\pi}{4}, n = 0, 1, \ldots, 7\} \]
  
  \[
  \begin{array}{c|c|c|c}
  |\uparrow\rangle & |\downarrow\rangle & |\leftarrow\rangle & |\rightarrow\rangle \\
  \hline
  |\uparrow\rangle & |\rightarrow\rangle & |\leftarrow\rangle & |\rightarrow\rangle \\
  |\rightarrow\rangle & |\uparrow\rangle & |\uparrow\rangle & |\rightarrow\rangle \\
  \end{array}
  \]

- Classical computation

- Alice gets the output

Input built into circuit

Classical input, classical output

Applies quantum operations and measurements

Classical Communication

Classical Communication

repeat
Our technique

- Derived from Measurement Based quantum computing (MBQC) [Raussendorf and Briegel, 2001]
- First time that a new functionality is achieved in MBQC.
The MBQC paradigm

How to convert any quantum circuit to MBQC:

1. Start with *cluster state*

2. Perform $\{|0\rangle, |1\rangle\}$-basis measurements, depending on position of CNOT gates in quantum circuit

3. Perform x-y plane measurements adaptively, layer by layer

Qubits are measured layer-by-layer…

Each qubit $j$ has a target measurement angle $\phi_j$

Measure in basis

$\{\frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi_j}|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - e^{i\phi_j}|1\rangle)\}$

Each edge a two-qubit interaction

$C - Z = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & -1
\end{pmatrix}$

$\phi'_j = (-1)^{s^j_x} \phi_j + \pi s^j_z$

$(s^j_x \in \{0, 1\} \text{ and } s^j_z \in \{0, 1\} \text{ depend on previous measurement outcomes})$
Getting rid of \{\ket{0}, \ket{1}\} basis measurements

- We want to get rid of computational basis measurements that reveal the structure of underlying circuit
- We’ll show that \hspace{1cm}

\[
\begin{array}{c}
\text{yields universal set of gates: CNOT, H, and } \pi/8 \\
\text{Tilling the 2-qubit gate allows multiple inputs and multiple gates}
\end{array}
\]
Getting rid of \{\ket{0}, \ket{1}\} -basis measurements

\[
\begin{array}{cccc}
0 & 0 & \frac{\pi}{2} & 0 \\
0 & \frac{\pi}{2} & 0 & -\frac{\pi}{2} \\
\frac{\pi}{2} & \frac{\pi}{2} & \frac{\pi}{2} & 0 \\
0 & 0 & 0 & 0
\end{array}
\]

\[
\begin{array}{cccc}
0 & 0 & \frac{\pi}{2} & 0 \\
0 & \frac{\pi}{2} & 0 & -\frac{\pi}{2} \\
\frac{\pi}{2} & \frac{\pi}{2} & \frac{\pi}{2} & 0 \\
0 & 0 & 0 & 0
\end{array}
\]

\[
\begin{array}{cccc}
0 & 0 & \frac{\pi}{2} & 0 \\
0 & \frac{\pi}{2} & 0 & -\frac{\pi}{2} \\
\frac{\pi}{2} & \frac{\pi}{2} & \frac{\pi}{2} & 0 \\
0 & 0 & 0 & 0
\end{array}
\]

= \[
\begin{array}{cccc}
0 & 0 & \frac{\pi}{2} & 0 \\
0 & \frac{\pi}{2} & 0 & -\frac{\pi}{2} \\
\frac{\pi}{2} & \frac{\pi}{2} & \frac{\pi}{2} & 0 \\
0 & 0 & 0 & 0
\end{array}
\]

= \[
\begin{array}{cccc}
0 & 0 & \frac{\pi}{2} & 0 \\
0 & \frac{\pi}{2} & 0 & -\frac{\pi}{2} \\
\frac{\pi}{2} & \frac{\pi}{2} & \frac{\pi}{2} & 0 \\
0 & 0 & 0 & 0
\end{array}
\]

= \[
\begin{array}{cccc}
0 & 0 & \frac{\pi}{2} & 0 \\
0 & \frac{\pi}{2} & 0 & -\frac{\pi}{2} \\
\frac{\pi}{2} & \frac{\pi}{2} & \frac{\pi}{2} & 0 \\
0 & 0 & 0 & 0
\end{array}
\]

= \[
\begin{array}{cccc}
0 & 0 & \frac{\pi}{2} & 0 \\
0 & \frac{\pi}{2} & 0 & -\frac{\pi}{2} \\
\frac{\pi}{2} & \frac{\pi}{2} & \frac{\pi}{2} & 0 \\
0 & 0 & 0 & 0
\end{array}
\]
Getting rid of \{ |0\>, |1\> \} -basis measurements

The *brickwork* states

2-qubit circuit

4-qubit circuit

\( n \)-qubit circuit…

All measurements are integer multiples of \( \frac{\pi}{4} \).
Blind QC Protocol

- prepares qubits randomly chosen in
  \( \{ \frac{1}{\sqrt{2}} (|0\rangle + e^{i\theta}|1\rangle) \mid \theta \in \{ \frac{\pi}{4}, n = 0, 1, \ldots, 7 \} \} \)
  \( |\uparrow\rangle \mid |\downarrow\rangle \mid |\leftrightarrow\rangle \mid |\leftrightarrow\rangle \mid |\rightarrow\rangle \mid |\rightarrow\rangle \mid |\leftarrow\rangle \mid |\leftarrow\rangle \mid |\uparrow\rangle \mid |\uparrow\rangle \mid |\rightarrow\rangle \mid |\rightarrow\rangle \)

- chooses x-y plane measurement angles, adaptively, layer by layer

\[ \delta = \phi' + \theta + \pi r \]

\[ \phi' = (-1)^{\delta_x} \phi + \pi \delta_z \]

- entangles according to brickwork state

- single-qubit measurements in basis

\( \{ \frac{1}{\sqrt{2}} (|0\rangle + e^{i\delta}|1\rangle), \frac{1}{\sqrt{2}} (|0\rangle - e^{i\delta}|1\rangle) \} \)

\[ r \text{ random. } r=1 \text{ flips Bob's measurement outcome. Alice can correct this.} \]
Privacy

- Intuitively, we want that from Bob’s point of view, all information received from Alice is independent of Alice’s input $X$.

- Bob does learn the dimensions of the brickwork state, giving an upper bound on the size of Alice's computation. He may also have some prior knowledge on $X$.

- Hence, we need to prove that Bob's view of the protocol does not depend on $X$, given his prior knowledge.
Privacy

- Formally:
  
  We say that a protocol is *blind while leaking at most* $L(X)$ if for any fixed $Y = L(X)$, the following two hold when given $Y$:
  
  1. The distribution of the classical information obtained by Bob is independent of $X$.
  2. The state of the quantum system obtained by Bob is fixed and independent both of $X$ and of the distribution of the classical information above.

- Theorem: Our protocol is blind, while leaking at most the dimensions of the brickwork state.
Let \( A \) be the quantum system initially sent from Alice to Bob.

Fix \( \vec{\delta} \). Because \( r \)'s are random, for each qubit of \( A \), one of the following two has occurred:

\[
\begin{align*}
    r &= 0 \quad \Rightarrow |\psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle + e^{i(\delta - \phi')}|1\rangle), \\
    r &= 1 \quad \Rightarrow |\psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle - e^{i(\delta - \phi')}|1\rangle).
\end{align*}
\]

Hence when \( r \) is unknown, \( A \) consists of copies of the two-dimensional completely mixed state, which is fixed and independent of \( \vec{\phi} \).

Let \( \vec{\phi} = (\delta_1, \delta_2, \delta_3, \ldots) \) be the classical information that Bob gets during the protocol.

Let \( \theta' = \theta + \pi r \) and \( \vec{\theta}' = (\theta_1', \theta_2', \theta_3', \ldots) \).

Let \( \theta' = \theta + \pi r \) and \( \vec{\theta}' = (\theta_1', \theta_2', \theta_3', \ldots) \).

Hence when \( r \) is unknown, \( A \) consists of copies of the two-dimensional completely mixed state, which is fixed and independent of \( \vec{\phi} \).

Hence \( \vec{\delta} = \vec{\phi} + \vec{\theta}' \).

\( \vec{\phi} \) is random, so \( \vec{\phi} \) and \( \vec{\theta}' \) are independent.

\[
\begin{align*}
    \delta &= \phi' + \theta + \pi r \quad \Rightarrow \\
    \phi' &= (-1)^{s_x} \phi + \pi s_z.
\end{align*}
\]
Detecting an interfering Bob

- Double the number of wires, randomly adding $N/2$ wires in $|0\rangle$ and $N/2$ wires in $|1\rangle$.
- An actively interfering Bob is caught with probability at least $\frac{1}{2}$. Repeat $s$ times.

We also have a fault-tolerant version that additionally provides authentication for quantum inputs and outputs.

For classical outputs that cannot easily be verified
Interactive proof

- The blind protocol is as an interactive proof for any problem in BQP.

It follows:

\[ \text{BQP} \subseteq \text{IP}_{\text{BQP}}^{\lvert \theta \rangle} \]

Trivially,

\[ \text{BQP} \supseteq \text{IP}_{\text{BQP}}^{\lvert \theta \rangle} \]

Hence,

\[ \text{BQP} = \text{IP}_{\text{BQP}}^{\lvert \theta \rangle} \]
Multi-prover interactive proofs

Cheating is detected by the authentication protocol

Our result:
\[ \text{BQP} \subseteq \text{MIP}^*_\text{BQP} \]

Trivially,
\[ \text{BQP} \supseteq \text{MIP}^*_\text{BQP} \]

Hence, \[ \text{BQP} = \text{MIP}^*_\text{BQP} \]

\[ \theta_j = \tilde{\theta}_j + m_j \pi \]

\[ \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \otimes N \]

\[ \{ \frac{1}{\sqrt{2}} (|0\rangle + e^{i\theta_j}|1\rangle), \frac{1}{\sqrt{2}} (|0\rangle - e^{i\theta_j}|1\rangle) \} \]
Open questions

- Is quantum communication required for blind quantum computation?

$IP_{BQP} \stackrel{?}{=} BQP$

Thank you